LISTING OF THE CLAIMS PER 37 C.F.R. §1.121

1-174. (Cancelled)

175. (Currently Amended) A method of redirecting data items from a messaging host system to a user's mobile device, comprising: ~~the steps of:~~

establishing a secure communications link between a ~~redirector host~~ computer system associated with the user and the user's mobile device;

~~generating~~ sending a first encryption key from the computer system associated with the user to [[at]] the redirector host system;

storing the first encryption key at the redirector host system;

~~generating a first decryption key at the redirector host system;~~

~~forwarding the~~ sending a first decryption key from the ~~redirector host system~~ computer system associated with the user to the user's mobile device using the secure communications link;

detecting a new data item for the user at the messaging host system by the redirector host system;

~~receiving a copy of the new data item at the redirector host system;~~

determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

if the new data item should be redirected, then encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

transmitting the encrypted new data item from the redirector host system to the user's mobile device.

176. (Currently Amended) The method as recited in claim 175, wherein ~~the step of~~ establishing a secure communications link between ~~a redirector host~~ the computer system associated with the user and the user's mobile device further comprises establishing a serial connection between ~~redirector host~~ the computer system associated with the user and the user's mobile device.

177. (Currently Amended) The method as recited in claim 175, wherein ~~the step of~~ establishing a secure communications link between ~~a redirector host~~ the computer system associated with the user and the user's mobile device further comprises using ~~Internet Message Access Protocol (IMAP) over~~ Secure Sockets Layer (SSL) protocol.

178. (Currently Amended) The method as recited in claim 175, wherein ~~the steps of generating a~~ sending the first encryption key ~~at the redirector host system~~ and ~~generating a~~ sending the first decryption key ~~at the redirector host system~~ further comprise generating a shared key.

179. (Currently Amended) The method as recited in claim 175, ~~wherein~~ further comprising generating the first encryption key and the first decryption key ~~are generated~~ according to a symmetric key encryption scheme.

180. (Currently Amended) The method as recited in claim 175, wherein ~~the step of generating a~~ sending the first encryption key ~~at the redirector host system~~ further comprises generating a public key.

181. (Currently Amended) The method as recited in claim 180, wherein ~~the step of generating a~~ sending the first decryption key ~~at the redirector host system~~ further comprises generating a private key.

182-183. (Cancelled)

184. (Currently Amended) The method as recited in claim [[182]] 175 further comprising~~:~~ ~~the steps of:~~

~~generating~~ sending a second decryption key from a computer system associated with the user to [[at]] the redirector host system;

storing the second decryption key at the redirector host system; and

~~generating a second encryption key at the redirector host system; and~~

~~forwarding the~~ sending a second encryption key from the computer system associated with the user ~~the redirector host system~~ to the user's mobile device using the secure communications link.

185. (Currently Amended) The method as recited in claim 184, wherein ~~the steps of generating a~~ sending the second encryption key ~~at the redirector host system~~ and ~~generating a~~ sending the second decryption key ~~at the redirector host system~~ further comprise generating a shared key.

186. (Currently Amended) The method as recited in claim 184, wherein sending the second encryption key and sending the second decryption key ~~are generated~~ further comprises generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

187. (Currently Amended) The method as recited in claim 184, wherein the ~~step of generating a~~ sending the second encryption key ~~at the redirector host system~~ further comprises generating a public key.

188. (Currently Amended) The method as recited in claim 187, wherein the ~~step of generating a~~ sending the second decryption key ~~at the redirector host system~~ further comprises generating a private key.

189. (Cancelled)

190. (Currently Amended) The method as recited in claim [[189]] 184 further comprising: ~~the steps of:~~

receiving [[the]] an encrypted [[reply]] data item from the user's mobile device at the redirector host system; and

decrypting the encrypted [[reply]] data item to recover the [[reply]] data item. ~~; and transmitting the reply data item to the messaging host system.~~

191. (Currently Amended) The method as recited in claim 190 further comprising the step of transmitting the [[reply]] data item to a destination system using an electronic address associated with the user at the messaging host system, wherein [[reply]] data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.

192. (Currently Amended) A system for redirecting data items from a messaging host system to a user's mobile device, comprising~~:~~ ~~the steps of:~~

a redirector host system operable to be connected to the messaging host system;

means for establishing a secure communications link between a ~~redirector host system~~ computer system associated with the user and the user's mobile device;

means for ~~generating~~ sending a first encryption key from the computer system associated with the user to [[at]] the redirector host system;

means for storing the first encryption key at the redirector host system;

~~means for generating a first decryption key at the redirector host system;~~

means for ~~forwarding the~~ sending a first decryption key from the ~~redirector host~~ computer system associated with the user to the user's mobile device using the secure communications link;

means for detecting a new data item for the user at the messaging host system by the redirector host system;

~~means for receiving a copy of the new data item at the redirector host system;~~

means for determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

means for encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

means for transmitting the encrypted new data item from the redirector host system to the user's mobile device.

193. (Currently Amended) The system as recited in claim 192, wherein the means for establishing a secure communications link between ~~a redirector host~~ the computer system associated withe the user and the user's mobile device further comprises a serial connection between ~~redirector host~~ the computer system associated with the user and the user's mobile device.

194. (Currently Amended) The system as recited in claim 192, wherein the means for establishing a secure communications link between ~~a redirector host~~ the computer system associated with the user and the user's mobile device further comprises means for using ~~Internet Message Access Protocol (IMAP) over~~ Secure Sockets Layer (SSL) protocol.

195. (Currently Amended) The system as recited in claim 192, wherein the means for ~~generating a~~ sending the first encryption key ~~at the redirector host system~~ and the means for ~~generating a~~ sending the first decryption key ~~at the redirector host system~~ further comprise means for generating a shared key.

196. (Currently Amended) The system as recited in claim 192, wherein the means for ~~generating a~~ sending the first encryption key ~~at the redirector host system~~ and the means for ~~generating a~~ sending the first decryption key ~~at the redirector host system~~ further comprise means for generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

197. (Currently Amended) The system as recited in claim 192, wherein the means for ~~generating a~~ sending the first encryption key ~~at the redirector host system~~ further comprises means for generating a public key.

198. (Currently Amended) The system as recited in claim 197, wherein the means for ~~generating a~~ sending the first decryption key ~~at the redirector host system~~ further comprises means for generating a private key.

199-200. (Cancelled)

201. (Currently Amended) The system as recited in claim [[199]] 192 further comprising:

means for ~~generating~~ sending a second decryption key from a computer system associated with a second user [[at]] to the redirector host system;

means for storing the second decryption key at the redirector host system; and

~~means for generating a second encryption key at the redirector host system; and~~

means for ~~forwarding the~~ sending a second encryption key from the ~~redirector host~~ computer system associated with the user to the user's mobile device using the secure communications link.

202. (Currently Amended) The system as recited in claim 201, wherein the means for ~~generating a~~ sending the second encryption key ~~at the redirector host system~~ and the means for ~~generating a~~ sending the second decryption key ~~at the redirector host system~~ further comprise means for senerating a shared key.

203. (Currently Amended) The system as recited in claim 201, wherein the means for ~~generating a~~ sending the second encryption key ~~at the redirector host system~~ and the means for ~~generating a~~ sending the second decryption key ~~at the redirector host system~~ further comprise means for generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

204. (Currently Amended) The system as recited in claim 201, wherein the means for ~~generating a~~ a second encryption key ~~at the redirector host system~~ further comprises means for generating a public key.

205. (Currently Amended) The system as recited in claim 204, wherein the means for ~~generating a~~ sending the second decryption key ~~at the redirector host system~~ further comprises means for generating a private key.

206. (Cancelled)

207. (Currently Amended) The system as recited in claim [[206]] 201 further comprising:

means for receiving [[the]] an encrypted [[reply]] data item from the user's mobile device at the redirector host system; and

means for decrypting the encrypted [[reply]] data item using the second decryption key to recover the [[reply]] data item. ~~; and means for transmitting the reply data item to the messaging host system.~~

208. (Currently Amended) The system as recited in claim 207 further comprising the means for transmitting the [[reply]] data item to a destination system using an electronic address associated with the user at the messaging host system, wherein [[reply]] data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.

209. (Currently Amended) A computer-accessible medium having a sequence of instructions which, when executed by a processing entity, effectuate redirection of data items from a messaging host system to a user's mobile device, the computer-accessible medium comprising:

~~a code portion~~ instructions for establishing a secure communications link between a ~~redirector host~~ computer system associated with the user and the user's mobile device;

~~a code portion for generating~~ instructions for sending a first encryption key from a computer system associated with the user to [[at]] the redirector host system;

~~a code portion~~ instructions for storing the first encryption key at the redirector host system;

~~a code portion for generating a first decryption key at the redirector host system;~~

~~a code portion for forwarding the~~ instructions for sending a first decryption key from the ~~redirector host system~~ computer system associated with the user to the user's mobile device using the secure communications link;

~~a code portion~~ instructions for detecting a new data item for the user at the messaging host system by the redirector host system;

~~a code portion for receiving a copy of the new data item at the redirector host system;~~

~~a code portion~~ instructions for determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

~~a code portion~~ instructions for encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

~~a code portion~~ instructions for transmitting the encrypted new data item from the redirector host system to the user's mobile device.

210. (Currently Amended) The computer-accessible medium as recited in claim [[35]] 209, wherein the ~~code portion~~ instructions for establishing a secure communications link between ~~a redirector host~~ computer system associated with the user and the user's mobile device further comprises ~~a code portion~~ instructions for establishing a serial connection between ~~redirector host~~ the computer system associated with the user and the user's mobile device.

211. (Currently Amended) The computer-accessible medium as recited in claim [[35]] 209, wherein the ~~code portion~~ instructions for establishing a secure communications link between ~~a redirector host~~ the computer system associated with the user and the user's mobile device further comprises ~~a code portion~~ instructions for using ~~Internet Message Access Protocol (IMAP) over~~ Secure Sockets Layer (SSL) protocol.

212. (Currently Amended) The computer-accessible medium as recited in claim 209, wherein the ~~code portions for generating a~~ instructions for sending the first encryption key ~~at the redirector host system~~ and ~~generating a~~ for sending the first decryption key ~~at the redirector host system~~ further comprise ~~a code portion~~ instructions for generating a shared key.

213. (Currently Amended) The computer-accessible medium as recited in claim 209, wherein the ~~code portions for generating a~~ instructions for sending the first encryption key ~~at the redirector host system~~ and ~~generating a~~ for sending the first decryption key ~~at the redirector host system~~ further comprise ~~a code portion~~ instructions for generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

214. (Currently Amended) The computer-accessible medium as recited in claim 209, wherein the ~~code portion for generating~~ instructions for sending a first encryption key ~~at the redirector host system~~ further comprises ~~a code portion~~ instructions for generating a public key.

215. (Currently Amended) The computer-accessible medium as recited in claim 214, wherein the ~~code portion for generating~~ instructions for sending a first decryption key ~~at the redirector host system~~ further comprises ~~a code portion~~ instructions for generating a private key.

216-217. (Cancelled)

218. (Currently Amended) The computer-accessible medium as recited in claim [[216]] 209 further comprising:

~~a code portion for generating~~ instructions for sending a second decryption key [[at]] from the computer system associated with the user to the redirector host system;

~~a code portion~~ instructions for storing the second decryption key at the redirector host system; and

~~a code portion for generating a second encryption key at the redirector host system; and~~

~~a code portion for forwarding the~~ instructions for sending a second encryption key from the ~~redirector host~~ computer system associated with the user to the user's mobile device using the secure communications link.

219. (Currently Amended) The computer-accessible medium as recited in claim 218, wherein the ~~code portions for generation a~~ instructions for sending the second encryption key ~~at the redirector host system~~ and ~~generating a~~ for sending the second decryption key ~~at the redirector host system~~ further comprise a code portion for generating a shared key.

220. (Currently Amended) The computer-accessible medium as recited in claim 218, wherein the ~~code portions for generating a~~ instructions for sending the second encryption key ~~at the redirector host system~~ and ~~generating a~~ for sending the second decryption key ~~at the redirector host system~~ further comprise ~~a code portion~~ instructions for generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

221. (Currently Amended) The computer-accessible medium as recited in claim 218, wherein the ~~code portion for generating a~~ instructions for sending the second encryption key ~~at the redirector host system~~ further comprises ~~a code portion~~ instructions for generating a public key.

222. (Currently Amended) The computer-accessible medium as recited in claim 221, wherein the ~~code portion for generating a~~ instructions for sending the second decryption key ~~at the redirector host system~~ further comprises ~~a code portion~~ instructions for generating a private key.

223. (Cancelled)

224. (Currently Amended) The computer-accessible medium as recited in claim [[223]] 218 further comprising:

~~a code portion~~ instructions for receiving [[the]] an encrypted [[reply]] data item from the user's mobile device at the redirector host system; and

~~a code portion~~ instructions for decrypting the encrypted [[reply]] data item to recover the [[reply]] data item. ~~, and a code portion for transmitting the reply data item to the messaging host system.~~

225. (Currently Amended) The computer-accessible medium as recited in claim 224 further comprising ~~a code portion~~ instructions for transmitting the [[reply]] data item to a destination system using an electronic address associated with the user at the messaging host system, wherein [[reply]] data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.